

FIG. 1

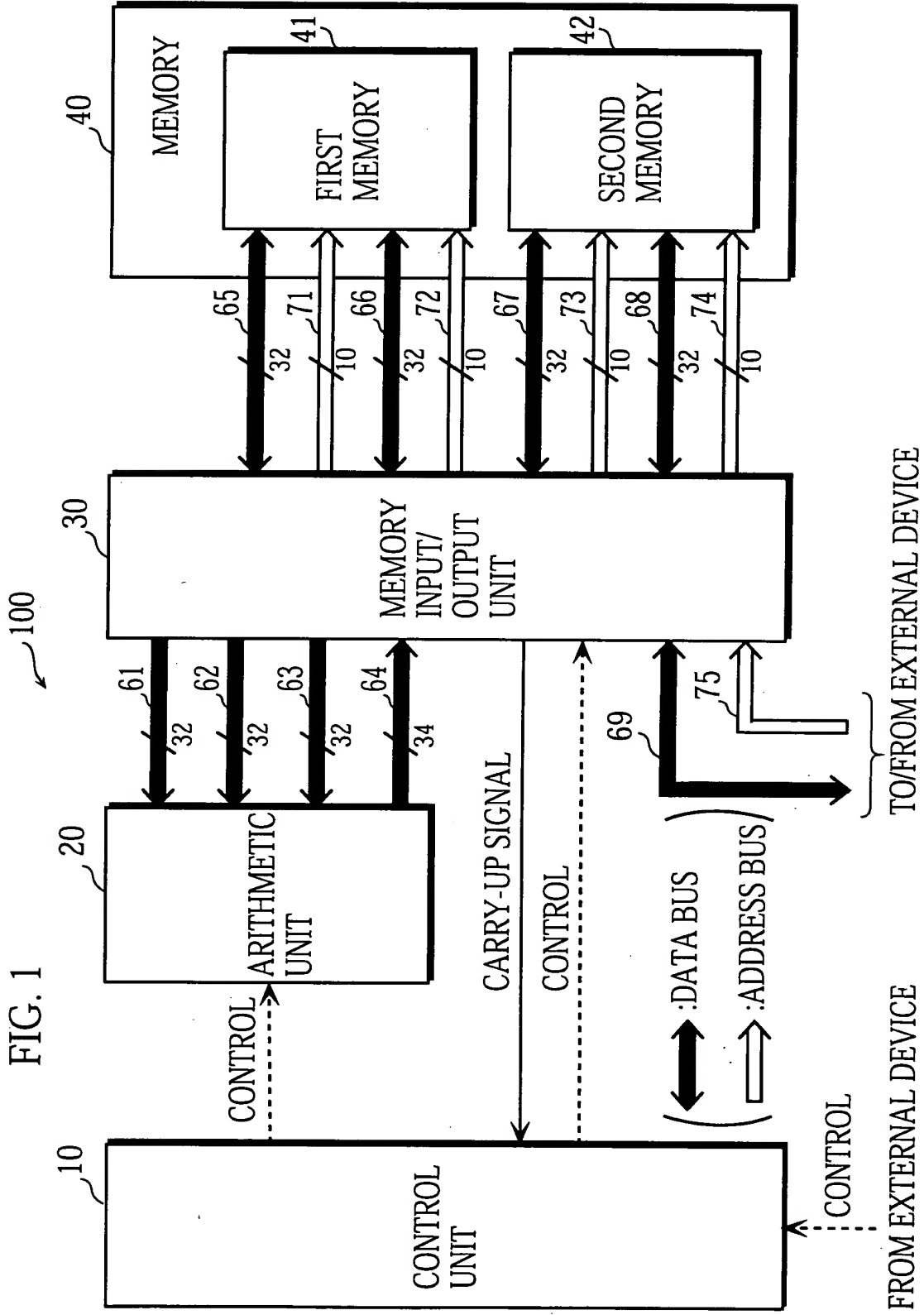


FIG. 2

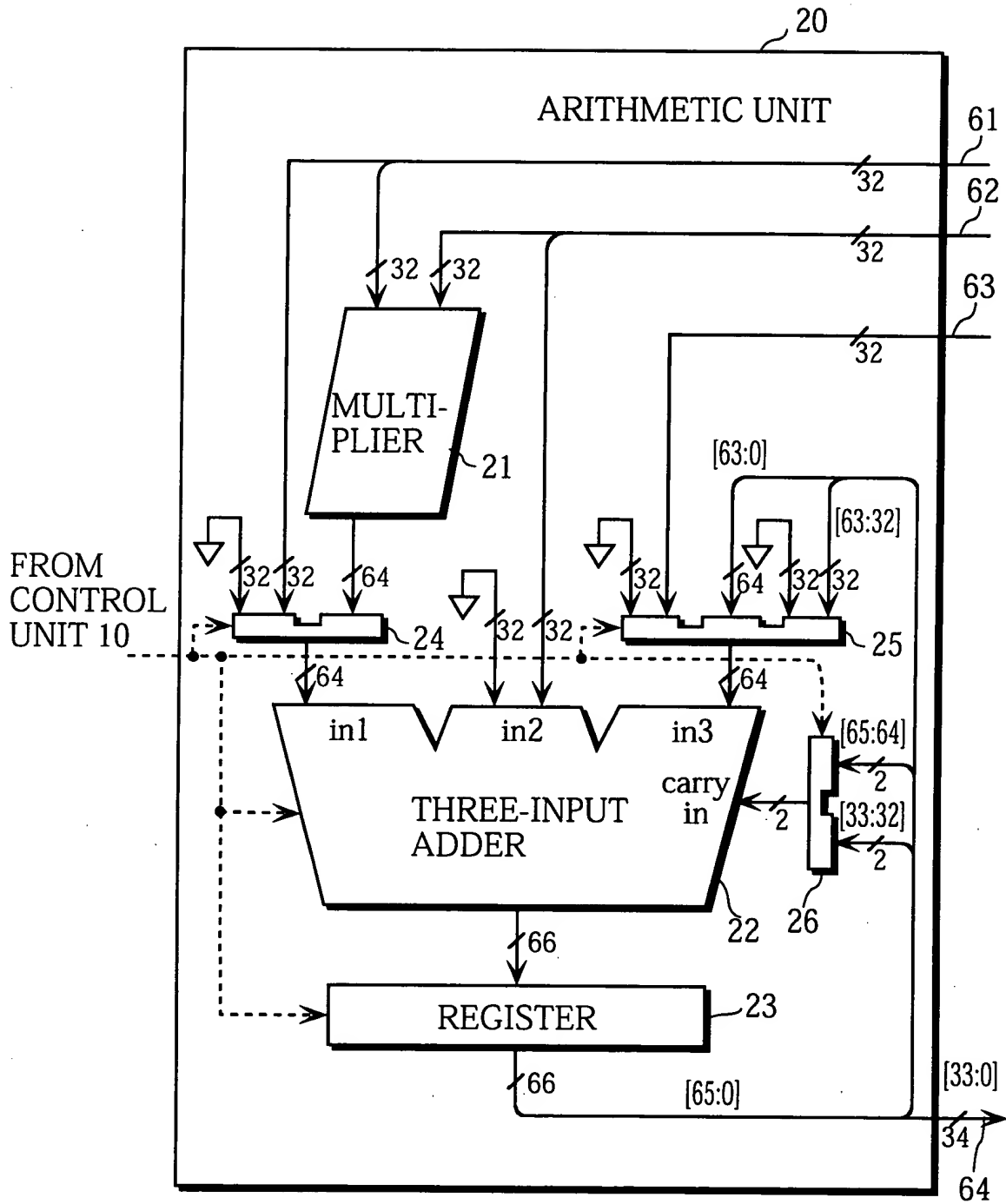


FIG. 3

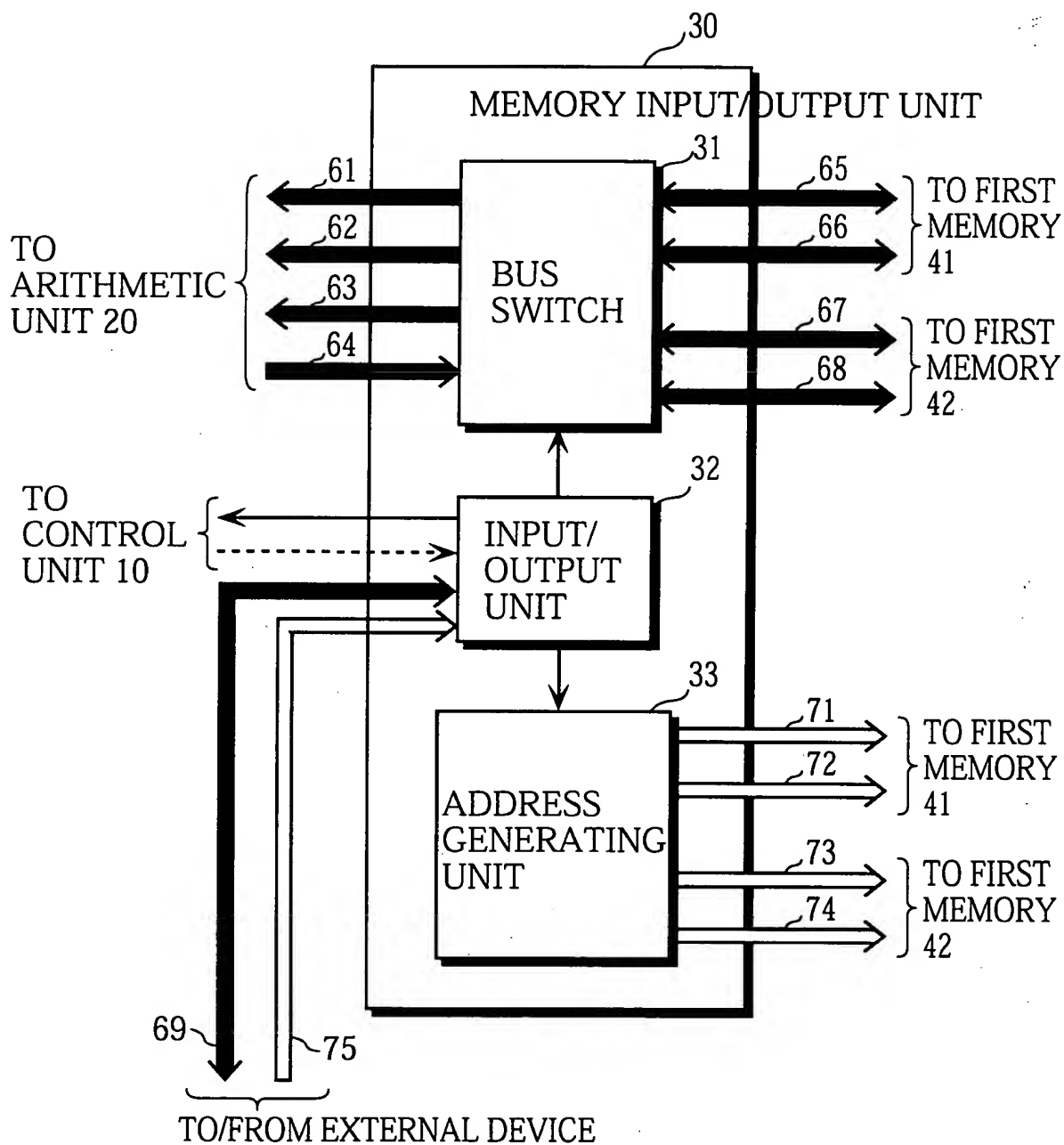


FIG. 4

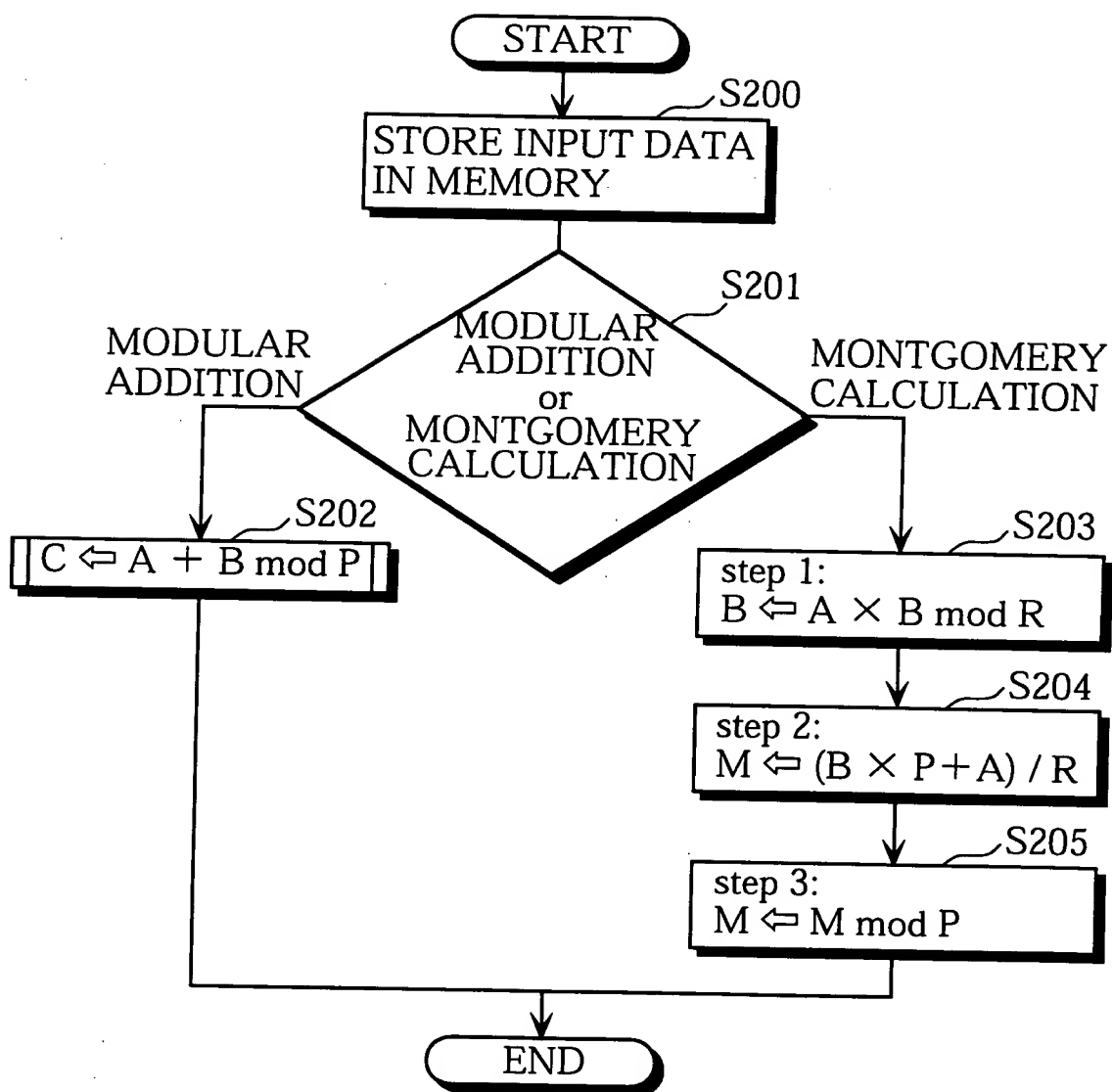




FIG. 6A

41

a0
a1
a2
a3
a4
.
.
p0
p1
p2
p3
p4
.
.
q0
q1
q2
q3
q4

FIG. 6B

42

b0
b1
b2
b3
b4
.
.
c0
c1
c2
c3
c4
.
.
w0
w1
w2
w3
w4

FIG. 7

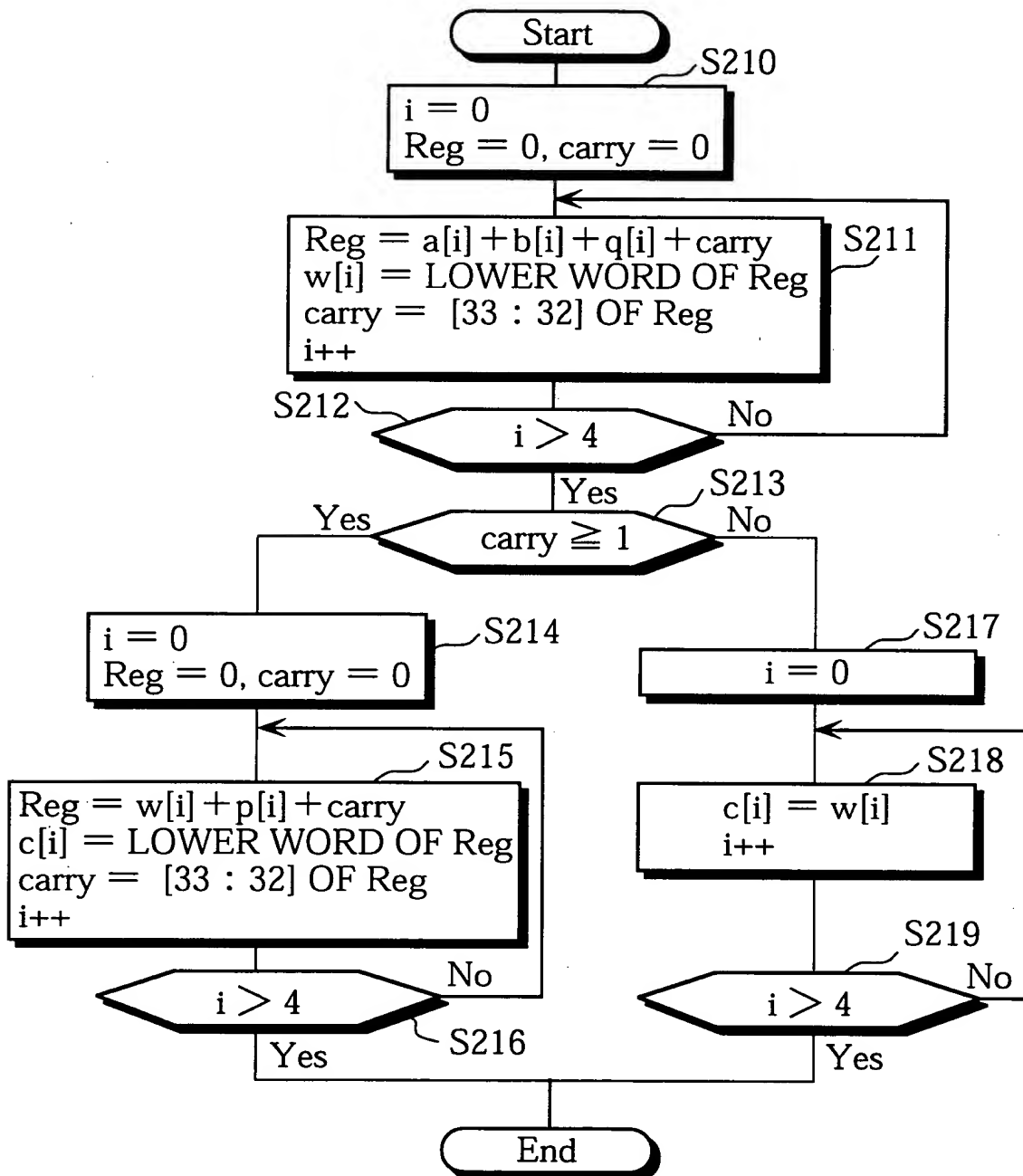


FIG. 8A

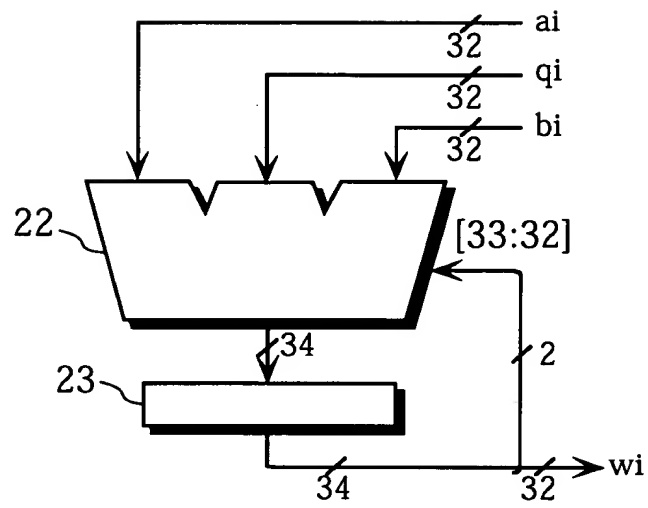


FIG. 8B

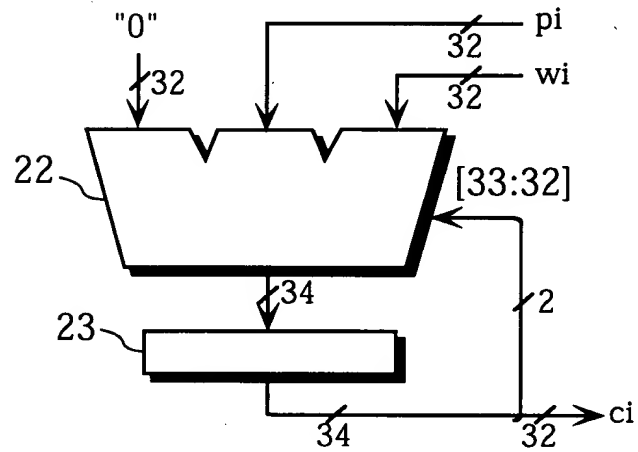
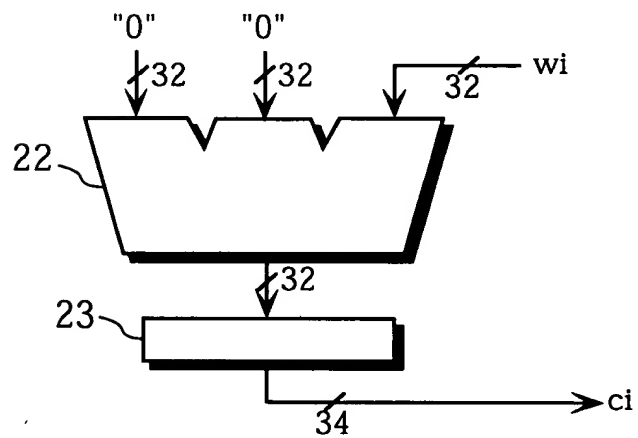


FIG. 8B





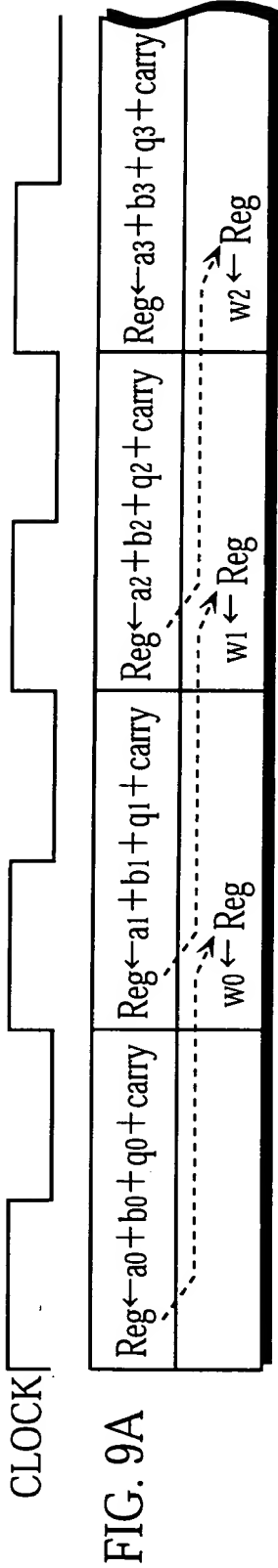


FIG. 9A

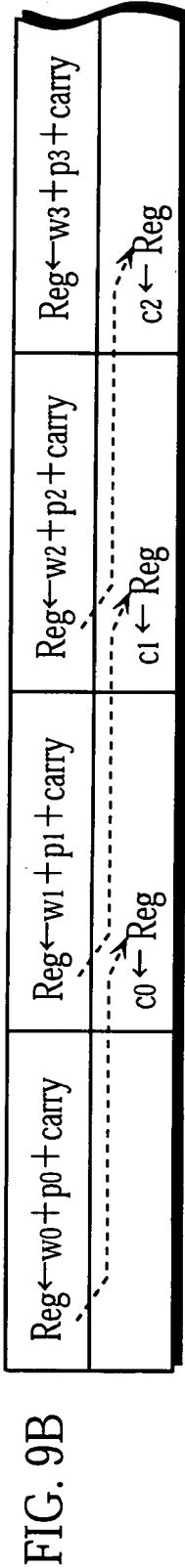


FIG. 9B

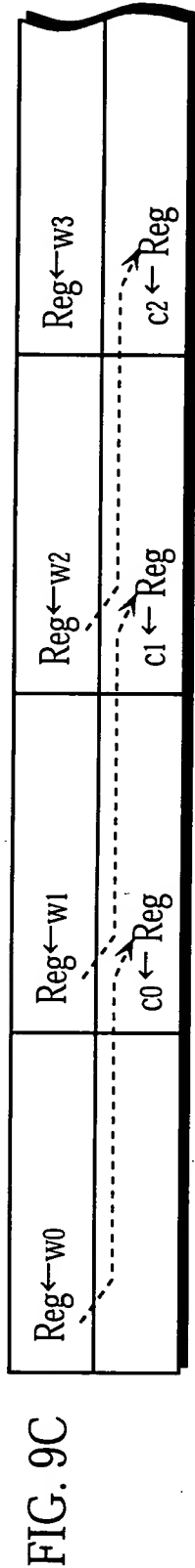


FIG. 9C

FIG. 10

	<p>INPUT : A</p> <p>PRECOMPUTATION : <math>V = -P^{-1} \bmod R</math> (<math>R = 2^{160}</math>)</p> <p>OUTPUT : <math>M = A \cdot R^{-1} \bmod P</math></p> <p>PROCESSING : step 1 <math>B = A \times V \bmod R</math></p> <p style="padding-left: 40px;">: step 2 <math>M = (B \times P + A) / R</math></p> <p style="padding-left: 40px;">: step 3 OUTPUT <math>M \bmod P</math></p>
<p>EXAMPLE INPUT</p>	<p>A: 10 · 010 · 011 · 101 · 111 · 010 · 101 · 000 · 101 · 010 · 111 · 0</p> <p>P: 10 · 010 · 101 · 000 · 101 · 1</p> <p>Q: 00 · 101 · 010 · 111 · 010 · 1</p> <p>V: 10 · 101 · 101 · 000 · 101 · 1</p>

FIG. 11A

a0
a1
a2
a3
a4
a5
a6
a7
a8
a9
.
.
p0
p1
p2
p3
p4
.
.
q0
q1
q2
q3
q4
.
.
m0
m1
m2
m3
m4

FIG. 11B

v0
v1
v2
v3
v4
v5
.
.
b0
b1
b2
b3
b4
.
.
c0
c1
c2
c3
c4
c5
.
.
e0(0xffffffff)
.
.
m0
m1
m2
m3
m4

FIG. 12A

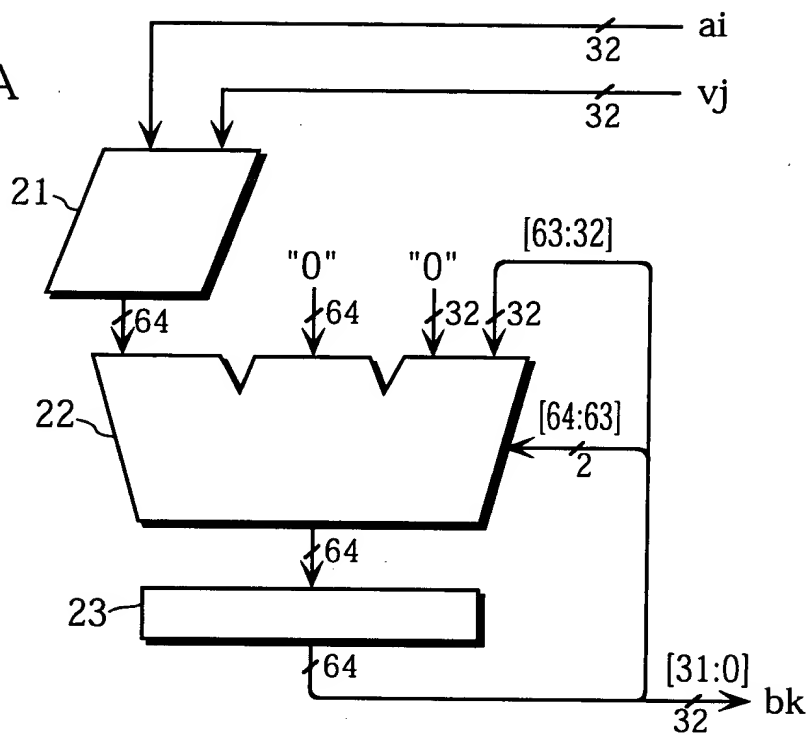


FIG. 12B

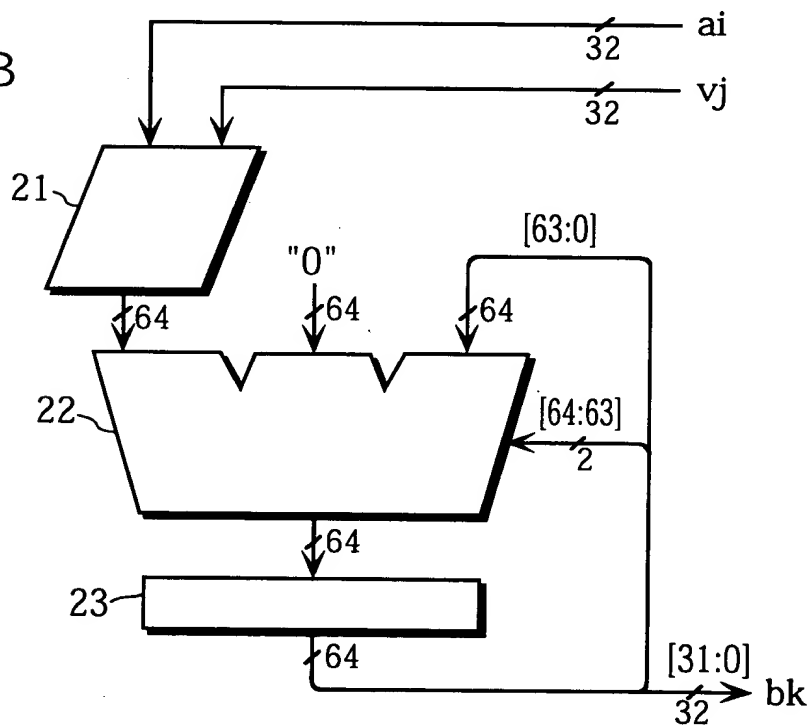


FIG. 13

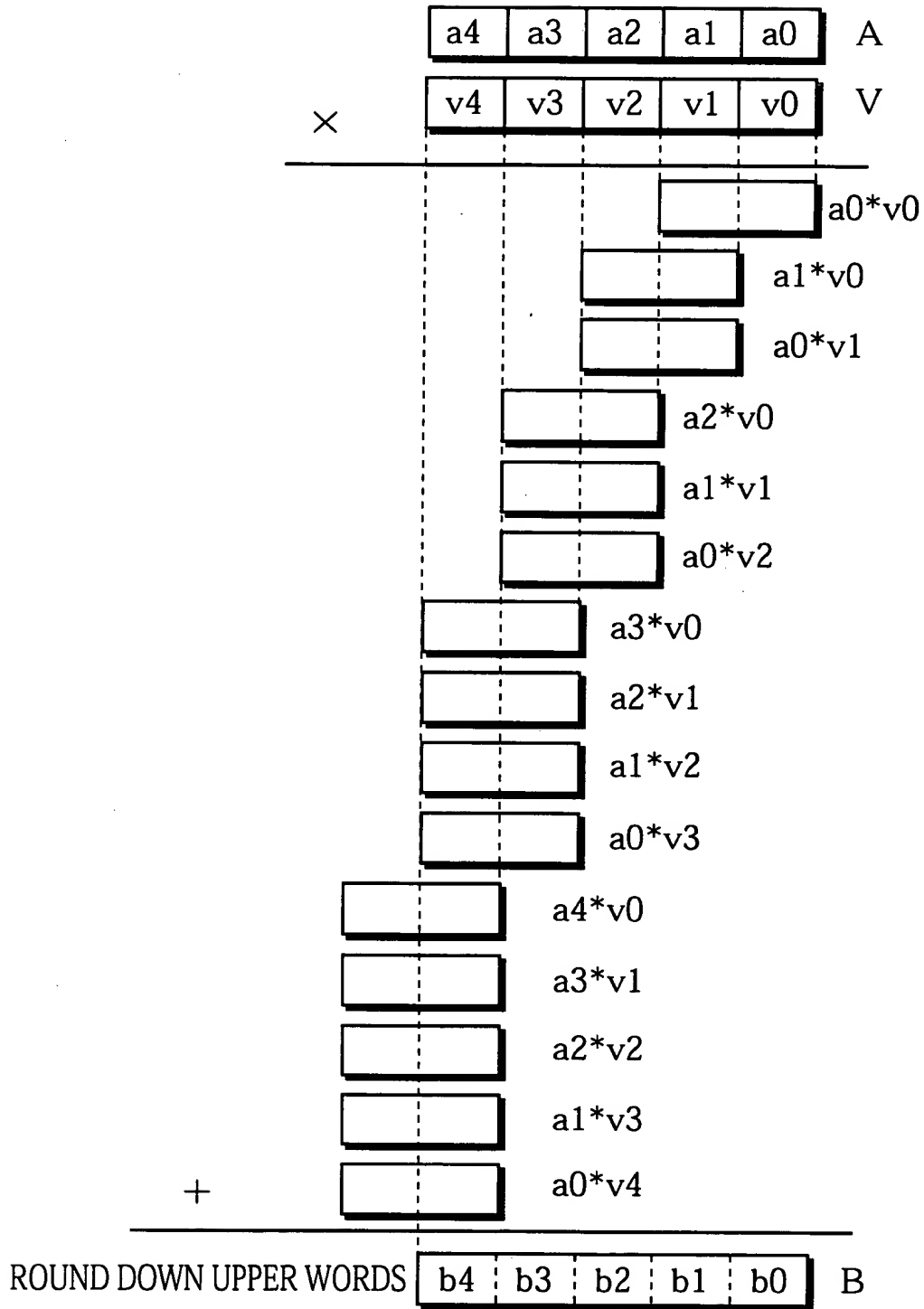


FIG. 14A

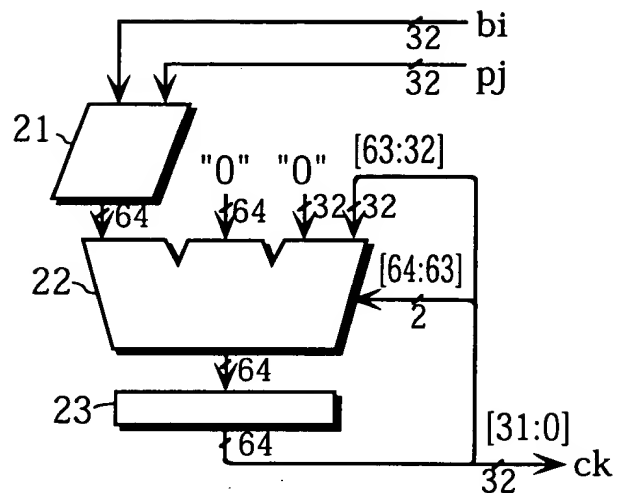


FIG. 14B

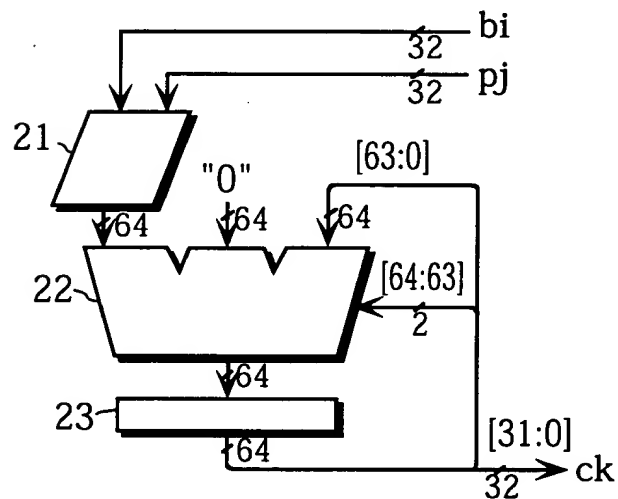


FIG. 14C

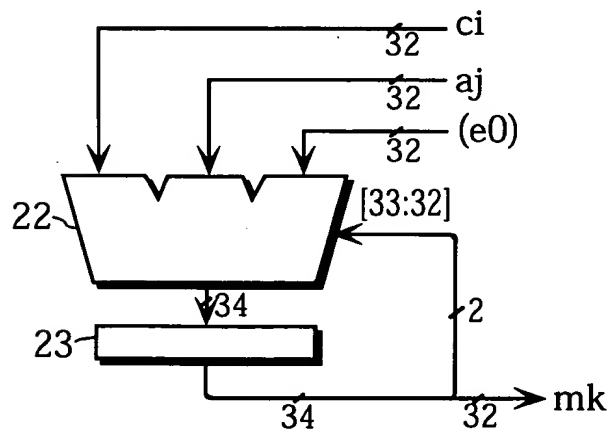


FIG. 15

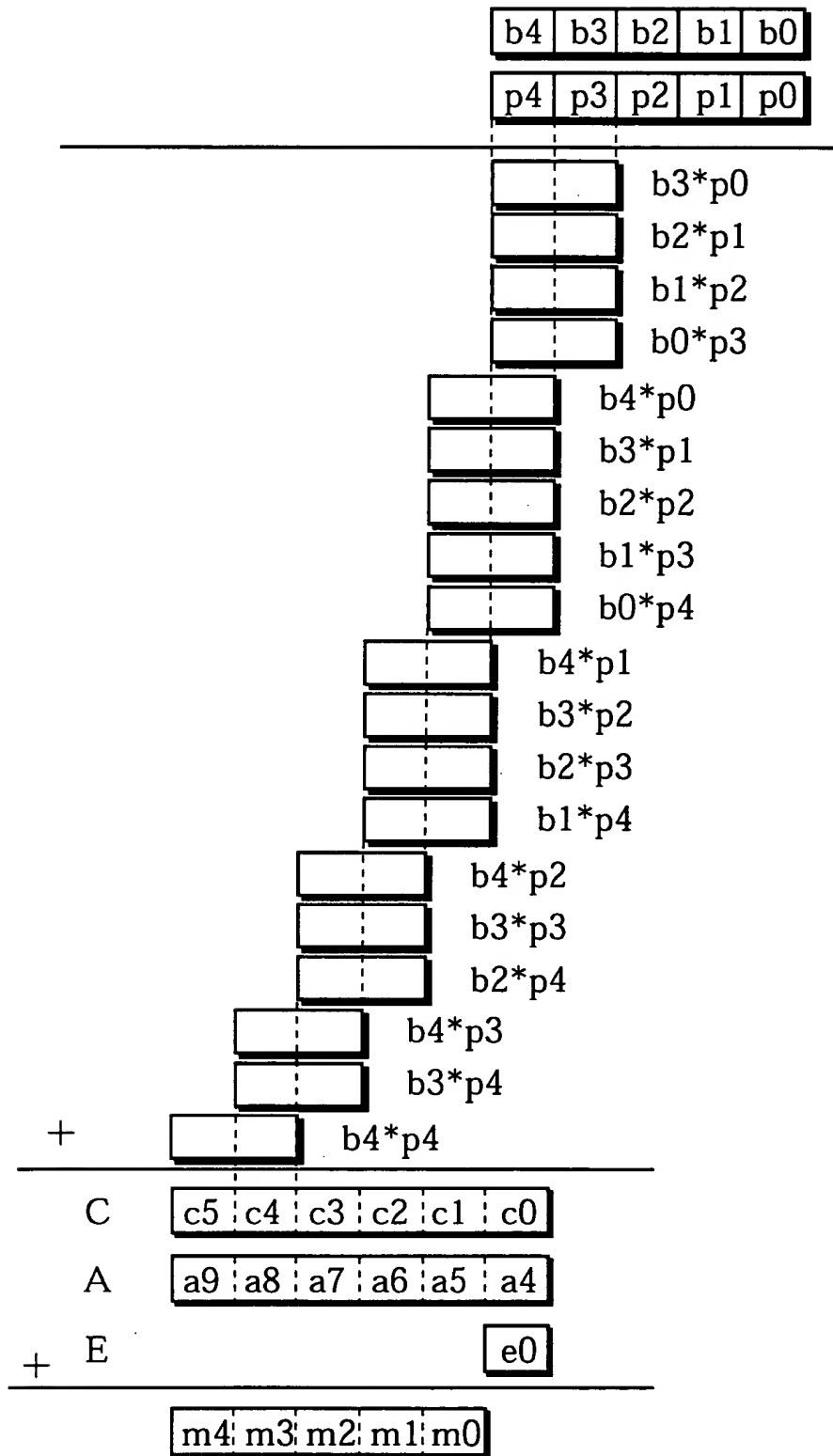


FIG. 16A

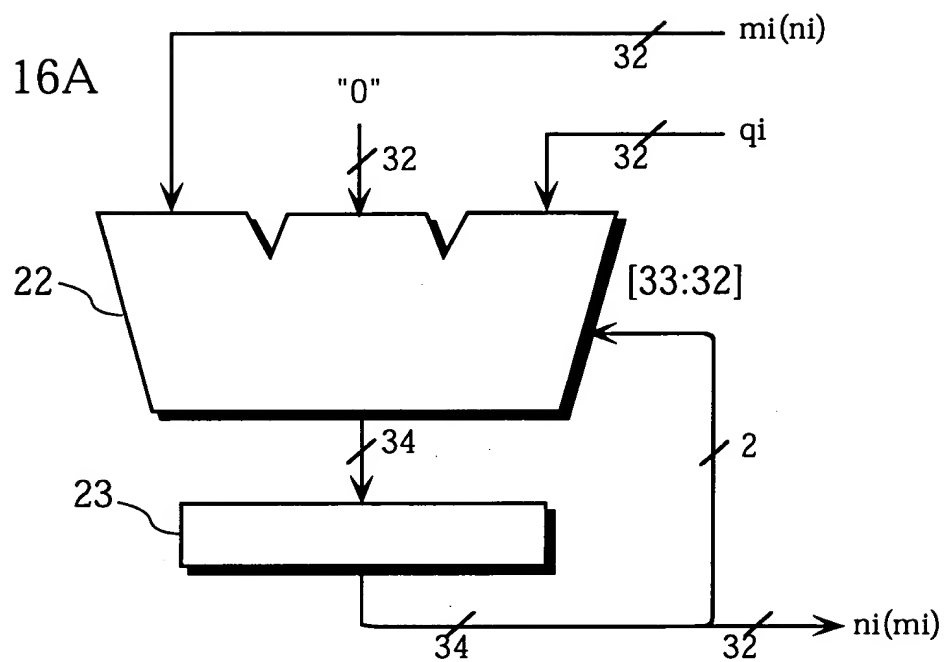


FIG. 16B

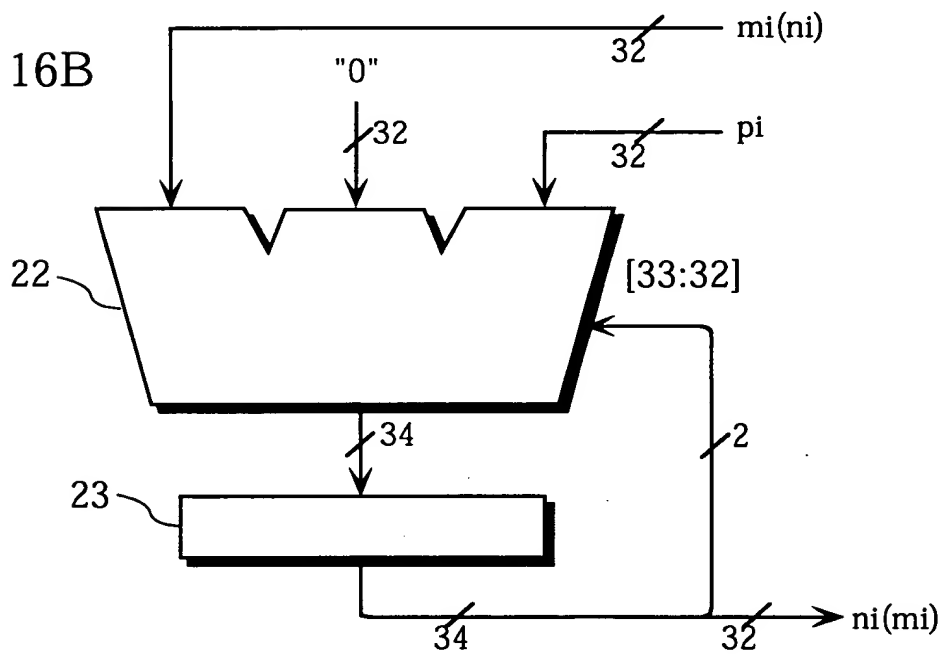




FIG. 17

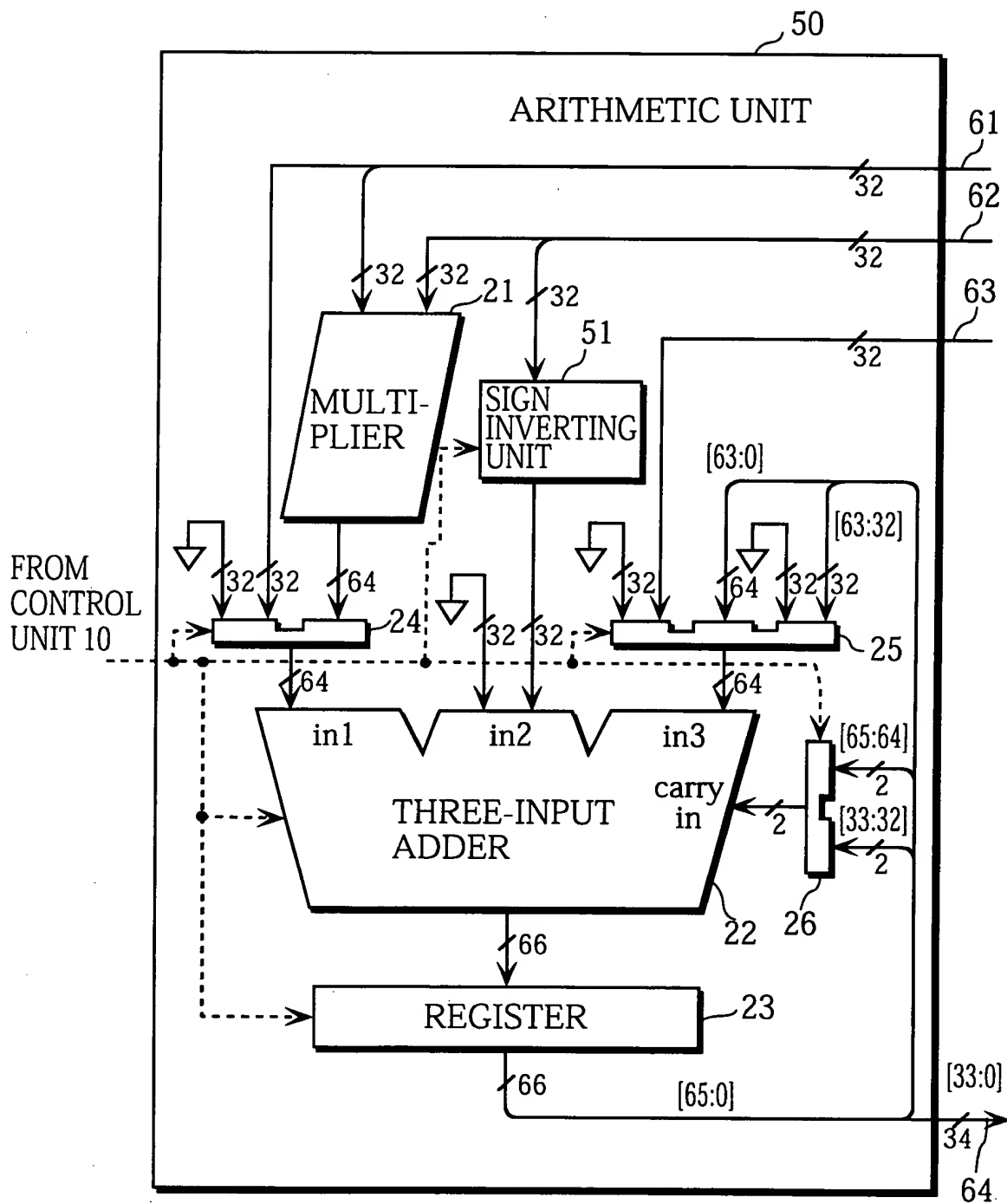


FIG. 18A

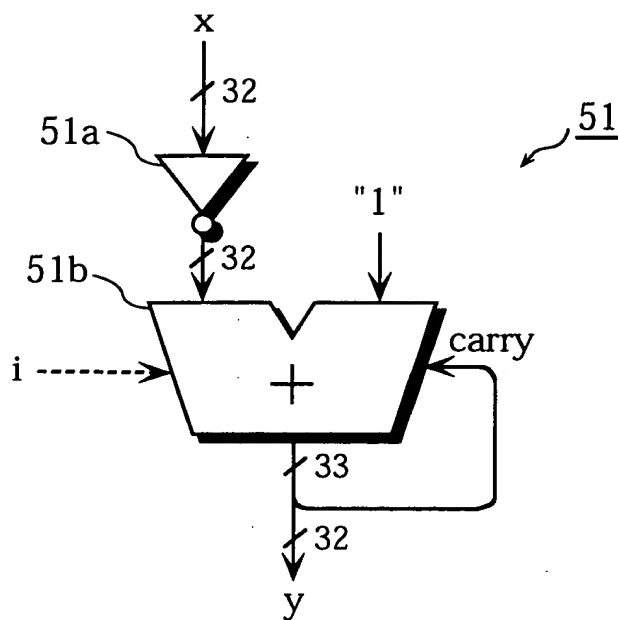


FIG. 18B

